# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-215255
(43)Date of publication of application : 04.08.2000

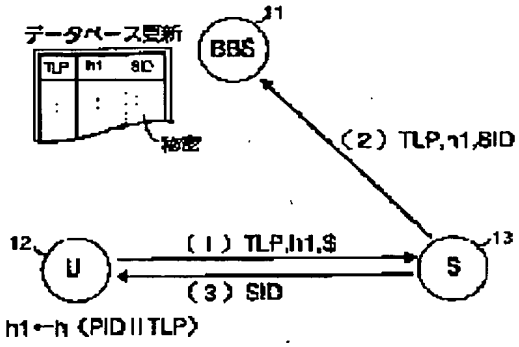
(51)Int.Cl. G06F 19/00
// G09C 1/00

(21)Application number : 11-012980
(22)Date of filing : 21.01.1999

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : MORITA HIKARI

## (54) METHOD AND DEVICE FOR PARTICIPATION TYPE LOTTERY

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent a sponsor from swindling winning money by the padding- out and to prevent a seller from embezzling a bet by generating hash values, for which the identifier and bedding pattern of a user are linked, with a hash function and requesting registration to a shop system while pairing these values.
SOLUTION: A user U generates a hash value h1=h(PID/TLP) with a hash function (h) from PID/TLP, for which information PID for identifying an individual and a bedding pattern TLP are linked at a user system, and requests the registration to a shop system 13 while pairing TLP and h1. The shop system 13 generates an identifier SID, transmits the SID to the user system 12 and transmits TLP, h1 and SID to a bulletin board system BBS 11. The bulletin board system BBS 11 manages TLP, h1 and SID in a data base while pairing them.




LEGAL STATUS

[Date of request for examination] 26.12.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－215255
（P2000－215255A）
(43)公開日　平成12年８月４日(2000.8.4)

| (51)Int.Cl.' | 識別記号 | ＦＩ | | テーマコード'（参考） |
|---|---|---|---|---|
| Ｇ０６Ｆ　19/00 | | Ｇ０６Ｆ　15/28 | Ｂ | ５Ｂ０４９ |
| // Ｇ０９Ｃ　1/00 | ６６０ | Ｇ０９Ｃ　1/00 | ６６０Ｇ | ５Ｊ１０４ |
| | | | ６６０Ｅ | ９Ａ００１ |

審査請求　未請求　請求項の数９　ＯＬ　（全８頁）

(21)出願番号　特願平11－12980

(22)出願日　平成11年１月21日(1999.1.21)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　森田　光
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100066153
弁理士　草野　卓　（外１名）

Ｆターム(参考)　5B049 BB11 BB37 BB46 CC39 EE03 EE05 FF03 FF04 GG04 GG07 GG10
5J104 AA07 KA01 KA03 KA05 NA05 NA12 NA36 PA00 PA12 PA17
9A001 EE02 EE03 JJ25 JJ76 KK60

(54)【発明の名称】　参加型くじ方法及びその装置

(57)【要約】
【課題】　安全性が高く、高速処理が可能で、主催者の当りくじ水増し、販売店の賭け金着服、ユーザのにせ当選金請求を排除する。
【解決手段】　ユーザＵはその識別子ＰＩＤと賭けパターンＴＬＰとの連結に対するハッシュ値ｈ１＝ｈ（ＰＩＤ‖ＴＬＰ）を求め、ｈ１とＴＬＰとお金を販売店Ｓへ送り、Ｓよりその識別子ＳＩＤを受領し、Ｓはｈ１，ＴＬＰの登録を掲示板ＢＢＳに対し行う、ＢＢＳはＴＬＰ，ｈ１，ＳＩＤを対としてデータベースで管理する。Ｕはｈ１の部分情報ｈ１* とＴＬＰをＢＢＳへ送り問い合わせ、一致したものがデータベースにあれば、ｈ１を返し、なければＵはＳＩＤを根拠に異議を申し立てる。ＵはＰＩＤを金融機関Ｂに提示し、Ｂはその賭けたｈ１と一致を確認して、当選金を支払う。

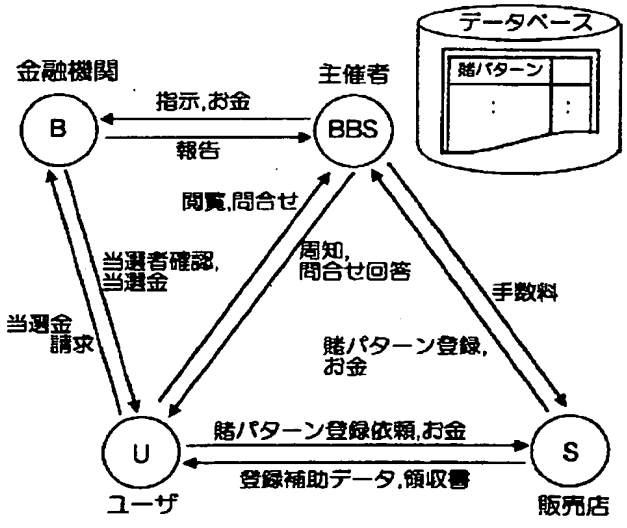



図１

【特許請求の範囲】

【請求項１】　掲示板装置と、ユーザの装置（以下ユーザ装置と記す）と、販売店装置と、金融機関装置とよりなり、

ユーザは上記ユーザ装置によりそのユーザを識別する情報ＰＩＤと賭けパターンＴＬＰとを連結し、その連結ＰＩＤ‖ＴＬＰからハッシュ関数ｈによってハッシュ値ｈ１＝ｈ（ＰＩＤ‖ＴＬＰ）を生成し、賭けパターンＴＬＰとハッシュ値ｈ１を対として販売店装置に登録依頼を行い、

販売店装置は上記登録依頼を受信すると、その販売店装置の識別子ＳＩＤを生成してユーザ装置に送信すると共に受信した賭けパターンＴＬＰとハッシュ値ｈ１とを掲示板装置へ送信し、

掲示板装置は受信した賭けパターンＴＬＰ、ハッシュ値ｈ１を対としてデータベースに管理し、複数のユーザからの賭けパターンＴＬＰが寄せられたら、その集計情報を公開し、

当選したユーザは掲示板装置に示された結果に従って、ユーザ装置により識別子ＰＩＤを示して金融機関装置に対して当選返戻金を請求し、

金融機関装置は当選返戻金請求を受けると、当選パターンが賭けパターンＴＬＰであり、それに賭けられたハッシュ値ｈ１が、受信識別子ＰＩＤから作られていることを確認して、当選返戻金をユーザへ渡すことを特徴とする参加型くじ方法。

【請求項２】　請求項１記載の方法において、

ユーザはユーザ装置により、上記ハッシュ値ｈ１の部分情報$h1^{*}$と賭けパターンＴＬＰを掲示板装置へ送信して自らの賭けパターンＴＬＰが存在することを問い合わせ、

この問い合わせを受けた掲示板装置は、問い合せた賭けパターンＴＬＰ及び部分情報$h1^{*}$と一致するものがデータベース中に在れば、そのハッシュ値ｈ１をユーザ装置へ返送し、一致するものがなければそのことをユーザ装置へ返送し、

一致するものなしの返送を受けたユーザ装置のユーザは掲示板装置と販売店装置に対して識別子ＳＩＤを根拠に異議申し立てをすることを特徴とする参加型くじ方法。

【請求項３】　請求項１記載の方法において、

販売店装置は上記登録依頼を受信した際に、販売店装置の識別子ＳＩＤを掲示板装置へ送信し、

掲示板装置は識別子ＳＩＤとハッシュ値ｈ１を連結し、その連結ＳＩＤ‖ｈ１に対するハッシュ値ｈ２＝ｈ（ＳＩＤ‖ｈ１）を生成し、ハッシュ値ｈ２を上記賭けパターンＴＬＰ、ハッシュ値ｈ１に対としてデータベースに管理し、

ユーザはユーザ装置により、受信した識別子ＳＩＤとハッシュ値ｈ１を連結し、その連結ＳＩＤ‖ｈ１に対するハッシュ値ｈ２＝ｈ（ＳＩＤ‖ｈ１）を生成し、そのハッシュ値ｈ２の部分情報$h2^{*}$と賭けパターンＴＬＰを掲示板装置へ送信して自らの賭けパターンＴＬＰが存在することを問い合わせ、

この問い合わせを受けた掲示板装置は、問い合せた賭けパターンＴＬＰ及び部分情報$h2^{*}$と一致するものがデータベース中に在れば、そのハッシュ値ｈ２をユーザ装置へ返送し、一致するものがなければそのことをユーザ装置へ返送し、

一致するものなしの返送を受けたユーザ装置のユーザは掲示板装置と販売店装置に対して識別子ＳＩＤを根拠に異議申し立てをすることを特徴とする参加型くじ方法。

【請求項４】　請求項１乃至３の何れかに記載の方法において、

掲示板装置は賭けパターン及びハッシュ値の公開リストに対し、掲示板装置の秘密の署名鍵で署名を生成し、その署名を上記公開リストに付けることを特徴とする参加型くじ方法。

【請求項５】　請求項１乃至４の何れかに記載の方法において、

ユーザ装置は上記ユーザ識別情報ＰＩＤに対しハッシュ値ｈ（ＰＩＤ）を求め、このハッシュ値ｈ（ＰＩＤ）と賭けパターンＴＬＰを連結し、この連結ｈ（ＰＩＤ）‖ＴＬＰを上記識別情報と賭けパターンの連結とし、

当選したユーザは識別子としてハッシュ値ｈ（ＰＩＤ）を金融機関装置へ送り、

金融機関装置は賭けられたハッシュ値ｈ１が受けとったハッシュ値ｈ（ＰＩＤ）から作られていることを確認し、その確認ができると、ユーザはＰＩＤを金融機関装置へ示し、賭けられたハッシュ値ｈ１が示されたＰＩＤから作られていることを確認して当選返戻金をユーザへ渡すことを特徴とする参加型くじ方法。

【請求項６】　参加型くじ方法に用いられるユーザ装置であって、

ユーザ識別子ＰＩＤなどを記憶する記憶部と、

入力手段と、

上記入力手段により入力された賭けパターンＴＬＰと上記ユーザ識別子ＰＩＤとを連結する連結手段と、

上記連結したユーザ識別子ＰＩＤと賭けパターンＴＬＰに対するハッシュ値ｈ１を求めるハッシュ関数手段と、

販売店装置からのその識別子ＳＩＤ、掲示板装置からの応答などを受信する受信手段と、

上記ハッシュ値ｈ１、上記賭けパターンＴＬＰを販売店装置へ、上記ハッシュ値ｈ１の部分情報$h1^{*}$及び上記賭けパターンＴＬＰを含む問い合わせを掲示板装置へそれぞれ送信する送信手段と、

を具備するユーザ装置。

【請求項７】　参加型くじ方法に用いられるユーザ装置であって、

ユーザ識別子ＰＩＤなどを記憶する記憶手段と、

入力手段と、

上記入力手段により入力された賭けパターンＴＬＰと上記ユーザ識別子とを連結する連結手段と、
上記連結したユーザ識別子ＰＩＤと賭けパターンＴＬＰに対するハッシュ値ｈ１を求めるハッシュ関数手段と、販売店装置からのその識別子ＳＩＤ、掲示板装置からの応答などを受信する受信手段と、
上記ハッシュ値ｈ１と上記識別子ＳＩＤとを連結する手段と、
上記連結したハッシュ値ｈ１と識別子ＳＩＤに対するハッシュ値ｈ２を求める手段と、
上記ハッシュ値ｈ１、上記賭けパターンＴＬＰを販売店装置へ、上記ハッシュ値ｈ２の部分情報ｈ２* 及び上記賭けパターンＴＬＰを含む問い合わせを掲示板装置へそれぞれ送信する送信手段と、
を具備するユーザ装置。
【請求項８】　請求項６又は７記載のユーザ装置において、
ユーザ識別子ＰＩＤに対しハッシュ関数をかけてハッシュ値ｈ（ＰＩＤ）を得るハッシュ関数手段を備え、
上記連結手段は、賭けパターンＴＬＰと上記ハッシュしたユーザ識別子ｈ（ＰＩＤ）とを連結する手段であり、
上記ハッシュ関数手段はハッシュしたユーザ識別子ｈ（ＰＩＤ）と賭けパターンＴＬＰとの連結に対してハッシュをかける手段であることを特徴とするユーザ装置。
【請求項９】　請求項６乃至８の何れかに記載のユーザ装置において、
掲示板装置から受信した公開リストの署名を、公開鍵で検証する署名検証手段を備えることを特徴とするユーザ装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、インターネットなど不特定多数の人々がアクセスできる環境下で、ゲームの結果などを対象にくじを投票し（賭け）公正に運用されるための参加型くじの方法及びそのユーザ装置に関する。ここで、参加型くじとは、競馬、競輪、競艇、ナンバーくじのたぐいのことであり、予め識別子が付され、くじが一意に定まっているものをユーザが購入するもの（例：宝くじ、宝くじ付年賀ハガキ）は、参加型くじの範囲には含まない。
【０００２】参加型くじの重要な特徴は、予め参加者であるユーザが結果を予想し、その予想したパターンのくじを購入することにある。予想パターンとゲーム結果などが一致すれば、当選したとして当選返戻金（以下、当選金）が主催者から支払われる。
【０００３】
【従来の技術】参加型くじのシステム構成を図１１に示す。参加型くじを主催する主催者と、ユーザＵと、販売店Ｓとよりなり、ユーザＵが賭けパターンを予想してくじの購入を、販売店Ｓにお金を支払って行い、販売店Ｓから、そのくじと、領収書を受領する。販売店Ｓはユーザより希望賭けパターンを主催者へ報告すると共にお金を送り、主催者から手数料を受取る。ユーザＵは当選くじを主催者に提示して当選金を主催者から受取る。
【０００４】主催者と販売者の所属組織が同一の場合が多い。なお、主催者による賭け対象（ゲームなど）の情報は、自らと報道を通じて周知され、賭け結果も同様に周知される。ここでのセキュリティ上の問題点は次のとおりである。くじの偽造は、紙とそれに印刷される印字の複製困難性により決まる。主催者および販売者の不正、それら組織の内部犯行による不正は法律などにより防止される。
【０００５】しかしながら、２０００年開始が決まっているサッカーくじなど、新しい参加型くじを考える場合、多数の参加者を想定するので、販売者と主催者は別個と考えざるを得ないので内部犯行防止対策の強化が必要である。また、インターネットなど不特定多数がアクセスできるネットワーク環境が普及しつつあるが、紙と印刷からなるくじを見直す必要がある。閉じたシステムならば従来通りで同様のセキュリティが維持できるが、関わる人が多いオープンなシステムの場合、くじを作る印字機そのものよりも、主催者・販売者を行き交う情報そのものに、安全性の対策を講じたものとすべきである。
参加型くじシステムの定義
ここで、参加型くじシステムが扱う参加型くじシステムは次の様なものとする。
・賭けパターンの予想を対象とする。
・投票券（以下、くじ）は、１口単位に投票可。
・当選返戻金（以下、当選金）は、１口単位に与えられる。但し、当選金の額は、主催者が決定する。
・販売店の組織は複数、当選金は一金融機関が扱う。
・購入者の身分（年齢、銀行口座、等）の確認手段がある。
・決済手段は別にある。
・夜間販売禁止にできる。
参加型くじシステムの構成
この発明が前提とする参加型くじシステムの構成を図１に示す。各エンティティ（主体）は、次のような役割を分担する。主催者は、くじの運営に関する全責任を持つとし、集めたお金の管理を金融機関Ｂに委託し、くじの販売は販売者Ｓに委託する。また、自ら、くじのデータを蓄えるデータベースと、くじの条件や対象とするゲームの結果と当選報告などを周知し、ユーザからの問い合わせにも応じる掲示板ＢＢＳを運営する。金融機関は、くじの売り上げを主催者から預かり、当選くじを持っているユーザＵの請求により、当選金を支払う。販売者はユーザからお金を貰って、ユーザの指示する賭けパターンを主催者に伝達する。くじを購入するユーザは、賭けるくじの条件などを、主催者の掲示板ＢＢＳなどから入

手し、くじの登録状況なども確認する。当選くじを持つユーザは金融機関に当選金を請求し、当選金を得る。なお、上記参加型くじシステムの定義のうち、夜間販売禁止は、システムの運用時間を設ければ解決するので以下の議論には含めない。

【０００６】

【発明が解決しようとする課題】上記の様な構成を前提に以下の項目をこの発明が解決しようとする課題とする。

Ａ．主催者の、水増しによる当選金横取り詐欺を防止する。

Ｂ．販売者の、主催者仲介をせず賭け金を着服する詐欺を防止する。

【０００７】Ｃ．ユーザ（くじ購入者）の、にせの当選金請求を排除する。

Ｄ．当選者のプライバシを確保すると共に、他人のなりすましを防止する。

【０００８】

【課題を解決するための手段】この発明によれば、ユーザはユーザ装置により、そのユーザの識別子ＰＩＤと賭けパターンＴＬＰを連結し、その連結したＰＩＤ‖ＴＬＰに対するハッシュ値ｈ１＝ｈ（ＰＩＤ‖ＴＬＰ）をハッシュ関数ｈによって生成し、ＴＬＰとｈ１をペアとして販売店装置に登録依頼し、販売店装置はその識別子ＳＩＤをユーザ装置へ送ると共に、ＴＬＰとｈ１とＳＩＤを掲示板装置へ送る。掲示板装置は受信したＴＬＰとｈ１とＳＩＤをペアとしてデータベースで管理し、ユーザ装置からｈ１の部分情報ｈ１$^{*}$とＴＬＰを掲示板装置へ送って、データベースに自らの賭けパターンＴＬＰが存在することを問い合わせ、この時、掲示板装置はＴＬＰとｈ１$^{*}$が一致するＴＬＰとｈ１があれば、そのｈ１を返し、自分の賭けパターンが自分のハッシュ値ｈ１と一緒に存在しなければ、ユーザは掲示板装置及び販売店装置に対してＳＩＤを根拠に異議申立てをする。掲示板装置はその集計情報を公開し、当選したユーザは掲示板装置により示された結果に従い、金融機関に対して当選返戻金を請求し、金融機関は当選パターンがＴＬＰであり、それに賭けられたハッシュ値ｈ１がユーザから渡された情報ＰＩＤから作られたことを確認してから、ユーザに当選金を渡す。

【０００９】主催者の掲示板装置により次のような時系列の管理を行う。

Phase Ⅰ　参加型くじの告示

－試合とその賭け方の周知。

Phase Ⅱ　経過処理

－統計情報の公開、登録データの更新。

【００１０】－個別問い合わせ回答（ユーザの登録確認）。

－夜間は販売店と示し合わせて休業。

Phase Ⅲ 投票確定（試合（ゲーム）の前に締切）

Phase Ⅳ　当選の案内（払戻し条件、等）

上記Ａ～Ｄの課題に対応して、以下の様な手段を導入する。

【００１１】一．（Ａ対策）試合開始前の賭条件確定の為、掲示板は公開情報ファイル全体に“随時ディジタル署名を付け公開”する。

二．（Ｂ，Ｃ対策）登録した自分のくじ（ハッシュ値）を問い合せの為に“部分ハッシュ”を使用する。

三．（Ｄ対策）当選者のプライバシ保護と内部犯行ガードの為、個人情報は“２重以上のハッシュ”で当選金手続き時の問い合せに呼応する。

【００１２】

【発明の実施の形態】参加型くじシステムの定義により、クレジット、電子マネー、またはデビットカード等で実現される。ここではどのようにするかの具体的手法は述べない。このとき、ネットワーク上に存在する、掲示板装置ＢＢＳ、販売者装置、ユーザ装置は次の様な関連をもって運用される。なお、金融機関Ｂとその他のエンティティＢＢＳおよびＵとの関係は、必ずしもネットワークで接続されている必要はない。とりわけ、当選金の支払処理は、オフラインを前提に以下の条件を進める。

Phase Ⅰ　参加型くじの告示

－掲示板装置ＢＢＳより、試合とその賭け方を周知させ、ネットワーク上に存在する多数のユーザＵ（必ずしもくじを買うことを必須としない）がこれを参照する。

Phase Ⅱ　経過処理（販売など）

－ユーザＵはそのユーザ装置によりネットワーク上で販売者Ｓの装置との間でくじを購買し、

－販売者Ｓからその販売者装置により掲示板装置ＢＢＳにくじの登録を依頼し、

－掲示板装置ＢＢＳは、くじの登録状況から、登録データの更新をするとともに統計情報を公開する。

【００１３】－ユーザＵよりそのユーザ装置により掲示板装置ＢＢＳへのくじ登録に関する個別問い合わせがあるとその回答をする（ユーザの登録確認）。

－夜間などは販売者と示し合わせて、販売を休止する。

Phase Ⅲ 投票確定（ゲーム（試合）の前に締切）

－掲示板装置ＢＢＳはデータベースの中身を凍結する。

Phase Ⅳ　当選の案内（払戻し条件、等）

－掲示板装置ＢＢＳから、当選の案内、支払条件の案内をする。

記号の凡例

・個人識別情報：ＰＩＤ

－一意のもの。例；銀行口座番号であり、対象とするゲームや対象の勝敗引きわけの賭けパターン毎に変化させるための乱数エリアを持つ。

・賭けパターン情報：ＴＬＰ

－主催者側が設定し、対象ゲーム毎に区別可能とされる。

・連結：X‖Y
－X‖Yは、Xの次にYを並べることを示す。
・ハッシュ関数：h ()
－h1←h（PID‖TLP）は入力PID‖TLPのハッシュ値をh1に代入することを示す。
・部分ハッシュ情報：$h^{\sharp}$
－$h^{\sharp}$ はハッシュ値hの一部分の値を示す。
・電子署名：sSKa（X）
－s1←sSKa（X）はaさんの秘密の署名生成鍵SKaでXに対して署名生成した署名をs1に代入すると読む。
【0014】－sSKa（X）はaさんの公開の署名検証鍵PKaでXに対して署名検証でき、正しい署名生成鍵SKaとXから生成された署名は有効と判断できる。従って、異なる署名生成鍵や入力Xの署名の場合、無効と判断される。－お金：＄電子的な金銭取引決済の流れを＄シンボルで表す。

第一の実施例

掲示板装置（BBS）11、ユーザUの装置（ユーザ装置）12、販売店Sの装置（販売店装置）13、金融機関Bの装置（金融機関装置）14からなるシステムにおいて、図2に示すようにユーザUはユーザ装置12により個人を識別する情報PIDと賭けパターンTLPより、PIDとTLPを連結したPID‖TLPからハッシュ関数hによってハッシュ値h1＝h（PID‖TLP）を生成し、TLPとh1をペアとして販売店装置13に登録依頼し、販売店装置13は識別子SIDを生成するとともに、ユーザ装置12にはSIDを、掲示板装置BBS11にはTLPとh1とSIDを送信する。
【0015】掲示板装置11は、TLPとh1とSIDをペアにデータベースに管理し、図3に示すようにユーザ装置12によりユーザUが上記h1の部分情報$h1^{\sharp}$とTLPを掲示板装置11へ送信することで、上記データベースに自らの賭けパターンTLPが存在することを問い合わせたとき、掲示板装置BBSはTLPとh1の一部と一致すれば、h1をユーザ装置12に返す。一方、自分の賭けパターンが自分のハッシュ値h1と一緒に存在しないときはそのことをユーザ装置12へ回答し、UはBBSとSに対して、SIDを根拠に異議申し立てをする。これは、上記第二の手段“部分ハッシュ”の使用のことである。
【0016】なお、前記問い合わせに対して、YesかNoだけで答えたとすると、答えに信ぴょう性がないのでh1 $^{\sharp}$ を送信し、h1を回答することにしている。掲示板装置BBS11は、複数のユーザから多数のTLPが寄せられたら、その集計情報を公開する。当選したユーザUは、掲示板装置BBS11により示された結果に従い、金融機関Bに対して図4に示すように情報PIDを渡し当選返戻金を請求し、金融機関Bはその装置14で、当選パターンがTLPであり、それに賭けられたハッシュ値h1が、Uから渡された情報PIDから作られることを確認してから、そのユーザUに当選返戻金を渡す。

第二の実施例

第一の実施例で、ユーザ装置よりh1の部分情報$h1^{\sharp}$を送って問い合わせを行ったが、第二の実施例では図5に示すように、SIDをh1とSIDの連結SID‖h1に対するハッシュ値h2＝h（SID‖h1）の部分情報$h2^{\sharp}$について問い合わせる。この場合は、掲示板装置11でハッシュ値h2＝h（SID‖h1）を作って、TLPとh2とh1とSIDをペアとしてデータベースで管理する。

第三の実施例

第一の実施例では掲示板装置11のデータベースのうち、TLPとh1に関するリストを公開したが、第三の実施例では、図6に示すようにその公開リスト情報に関して、掲示板装置11が秘密の署名鍵$SK_{BB}$で署名して公開する。これは、上記、第一の対策手段である。

第四の実施例

第一の実施例においてはユーザ装置12により、個人情報PIDと賭けパターンTLPより、PIDとTLPを連結したPID‖TLPからハッシュ関数hによってハッシュ値h1＝h（PID‖TLP）を生成した。この代わりに第四の実施例では図7に示すように、個人情報PIDのハッシュ値h（PID）とTLPを連結したh（PID）‖TLPからハッシュ関数hによってハッシュ値h1＝h（h（PID）‖TLP）を生成する。
【0017】ユーザUが当選したとき、金融機能Bは図8に示すように当選パターンがTLPであり、それに賭けられたハッシュ値h1が、ユーザUから渡された情報h（PID）から作られることを確認することを第一段階の確認とし、第二段階でPID自身を渡して確認させる。この実施例は、上記第三の手段“2重以上のハッシュ”を用いることである。
【0018】図8で示した例は、2重ハッシュの場合であるが、金融機関Bが出張所、支店、本店と階層に分かれている場合、例えば3重ハッシュにし、問い合わせの階層が上る度に、よりハッシュが掛かってないハッシュに落として照合する。また、ハッシュ値多重では、h（h（PID‖TLP′）‖TLP）、h（h（h（PID‖TLP″）‖TLP′）‖TLP）の様に、付加的な情報TLP′，TLP″を掲示板装置の指示の下、安全性を強化することができる。
【0019】上述したユーザ装置12の機能構成を図9に示す。記憶部21には識別子PIDの他、識別子SID、ハッシュ値h1、署名検証用公開鍵$PK_{BB}$などが記憶される。キーボードなどの入力手段22により賭けパターンTLPなどを入力することができ、連結部23でPIDとTLPが連結され、その連結はハッシュ関数部

２４でハッシュ値ｈ１が求められ、ｈ１，ＴＬＰは送信部２５より販売店装置へ送られる。またハッシュ値ｈ１の部分情報$h1^{*}$とＴＬＰが送信部２５により掲示板装置へ送られ、問い合わせが行われる。受信部２６にて販売店装置からＳＩＤを受信し、また、掲示板装置から公開リスト署名を受信し、公開リスト署名は署名検証部２７にて公開鍵$PK_{BB}$により検証される。

【００２０】第二の実施例の場合は、ＳＩＤとｈ１とが連結部２８で連結され、その連結に対しハッシュ値ｈ２がハッシュ関数部２９で求められ、そのｈ２の部分情報$h2^{*}$とＴＬＰが送信部２５より掲示板装置へ送られて問い合わせが行われる。またくじの購入ごとにＰＩＤに乱数を付加する場合は、乱数生成部３１から乱数Ｒを生成し、これを連結部２３へ入力して、ＰＩＤと連結させればよい。

【００２１】ＰＩＤをハッシュして用いる場合の例を図１０に示す。記憶部２１のＰＩＤを必要に応じて連結部３２で乱数Ｒと連結し、その連結ＰＩＤ‖Ｒに対するハッシュ値ｈ（ＰＩＤ‖Ｒ）をハッシュ関数部３３で求め、このハッシュ値ｈ（ＰＩＤ‖Ｒ）とＴＬＰを連結部２３で連結し、その連結に対するハッシュ値ｈ１をハッシュ関数部２４で求める。その他は図９の場合と同様である。

【００２２】

【発明の効果】上記各種実施例によれば、安全性が高く、速度性能において電子署名よりも効率の良いハッシュ関数をくじに用いることで、参加型くじシステムを構築することが出来る。また、くじを購買するユーザ個人にとっては、ハッシュ関数の計算の他は、ハッシュ値やＳＩＤを控えておく程度ですむ。従って、ハッシュ関数は、街頭や喫茶店（サイバーカフェ）にある公共端末やネットワーク接続のパソコンで生成してもらい、控えとして、紙にメモするか、プリンタから印字する環境で構築できる。従来とは異なり、仮にこの控えが盗まれたり複製されても、個人情報ＰＩＤが前提であるのでこれを知らなければ、他人が得てもなんら意味を持たないからである。

【００２３】掲示板装置の公開リスト署名を、ユーザの一部の有志がチェックすることにより、試合（ゲーム）結果が明らかになった後に主催者が当りくじを水増しするのを妨げることができる。ユーザが掲示板装置に問い合わせをすることにより、販売店での購入金着服に対するチェックをすることができる。

【図面の簡単な説明】

【図１】この発明の参加型くじシステムの構成を示す図。

【図２】くじ購買の手順を示す図。

【図３】登録確認の手順を示す図。

【図４】当選金受領の手順を示す図。

【図５】ＳＩＤによる登録確認の手順を示す図。

【図６】登録簿署名の例を示す図。

【図７】くじ購買（２重ハッシュ関数利用）の他の手順を示す図。

【図８】当選金受領（２重ハッシュ関数利用）の他の手順を示す図。

【図９】ユーザ装置の機能構成例を示す図。

【図１０】ユーザ装置の機能構成の他の例を示す図。

【図１１】従来のシステムを示す図。

【図１】

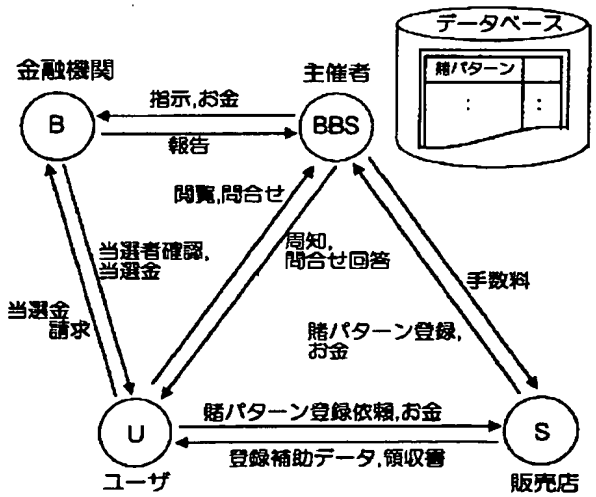



図１

【図２】

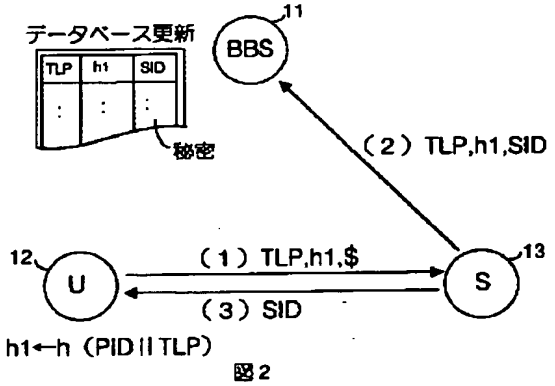



図２

【図３】

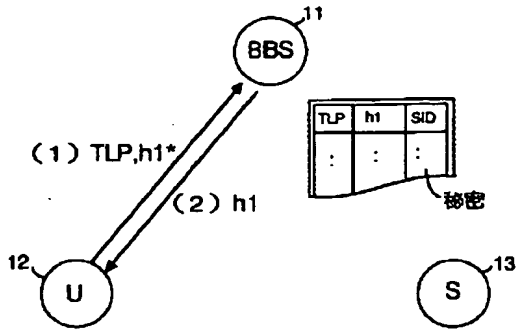



図３

【図４】

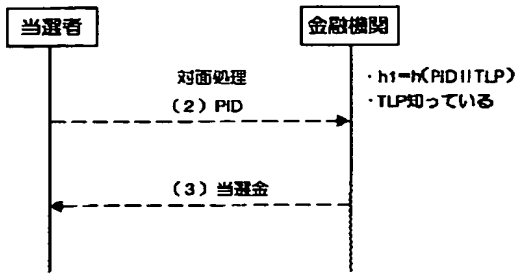



図４

【図５】

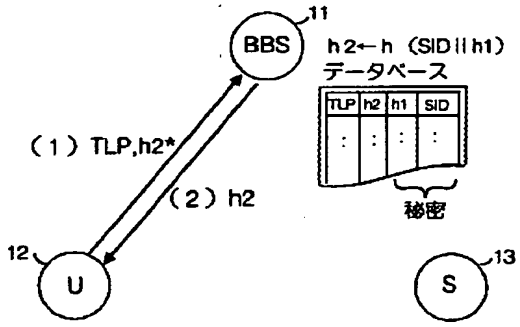



図５

【図６】

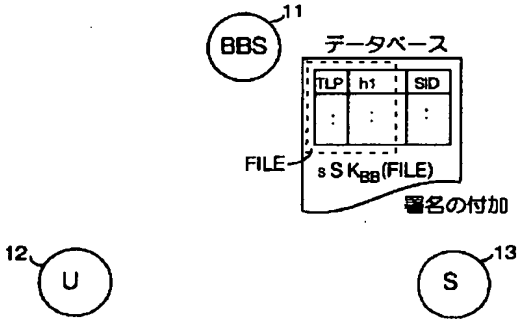



図６

【図７】

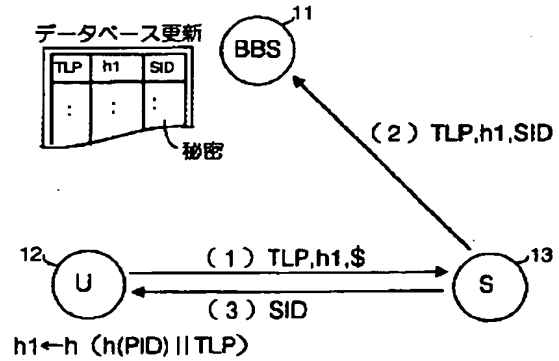



図７

【図８】

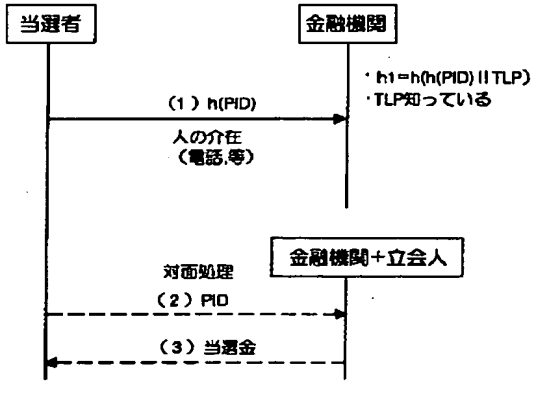



図８

【図９】

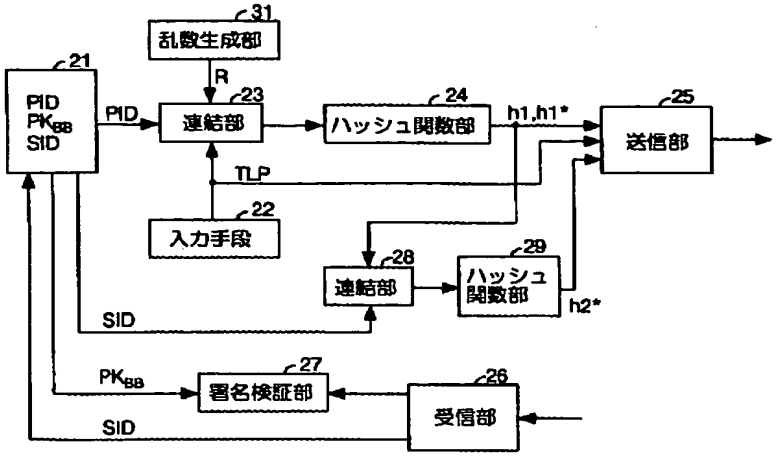



図９

【図１０】

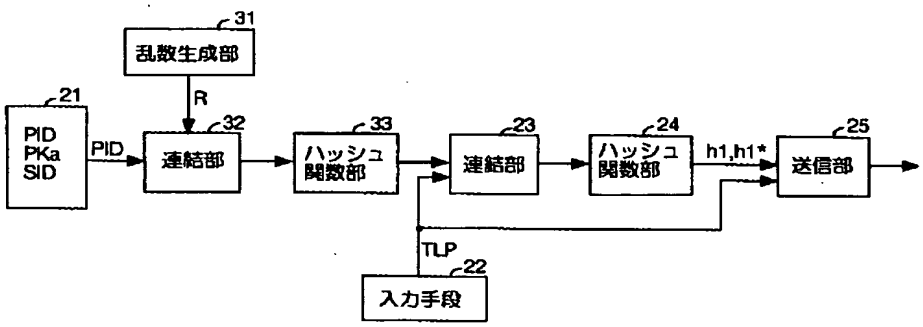



図１０

【図１１】

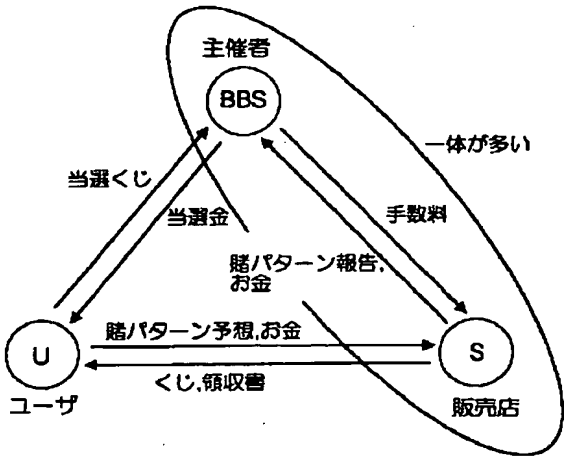



図１１